chinaXiv:201804.02035v1

可实现隐私保护的基于属性密文可搜索方案 *

胡媛媛，陈燕俐，朱敏惠

(南京邮电大学 计算机学院，南京 210003)

摘　要：针对现有的基于属性的密文可搜索方案存在隐私泄露问题以及当授权用户不在线时如何安全有效地将密文以及搜索权限委托给其他人的问题进行了研究，将隐藏访问结构的基于属性密文可搜索方案与代理重加密技术融合，提出了具有部分隐藏访问结构的支持代理重加密的功能的基于属性的密文检索方案。该方案不仅有效地解决了上述问题，而且还支持关键字的更新。最后在随机预言模型下基于 DL(D-linear)假设和 q-BDHE (decisional q-parallel bilinear Diffie-Hellman exponent)假设，证明了本方案的安全性。

关键词：云计算；基于属性的可搜索加密；隐藏访问结构；代理重加密

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2017.12.0760

Privacy protection attribute-based ciphertext search scheme

Hu Yuanyuan, Chen Yanli, Zhu Minhui

(*School of Computer Science*, *Nanjing University of Posts & Telecommunications*, *Nanjing* 210003, *China*)

Abstract: There are lots of drawbacks in existing attribute-based encryption with keyword search scheme, such as privacy disclosure issues and when the authorized user is offline how effectively delegate decrypt and search right to other people. In order to solve these problems, this paper proposed an attribute-based ciphertext search scheme with hidden access structures, which support proxy re-encryption function by combing attribute-based encryption with hidden access structures and proxy re-encryption technology. This scheme not only effectively solves the problems mentioned above, but also supports the update of keywords. Finally, under the random oracle model, the researchers proved the security of the scheme based on DL (D-linear) and q-BDHE (decisional q-parallel bilinear Diffie-Hellman exponent) hypothesis.

Key Words: cloud computing; attributed-based encryption with keyword search; hidden access structures; proxy re-encryption

0　引言

随着大数据和云计算的时代的到来，已经有越来越多的个人和企业都将大量私有数据上传到云系统，从而节省本地的存储和管理成本。为了保证数据的安全性，数据拥有者需要将数据加密后再上传到云系统中。2000 年，Song 和 Wagner 等人[1]第一次提出了可搜索加密(Searchable Encryption, SE)，实现了在不解密密文的情况下，能够利用关键字对密文进行快速检索。在实际应用中，一些数据需要被多个用户所共享，因此基于属性的可搜索加密方案引起众多学者的关注。相比于基于身份的可搜索加密，基于属性的可搜索加密不需要知道搜索者的具体身份信息，而是掌握搜索者的一系列的属性描述，当用户的属性满足密文中的访问结构才可进行搜索操作。因此，基于属性的可搜索加密能够实现细粒度的访问控制和密文。但是目前基于属性的可搜索加密中会将用户结构和搜索关键字发送给用户，而访问结构中包含了一些敏感信息，存在用户信息泄露的风险。

此外在实际应用中，数据共享时存在一些局限性，比如在医疗云系统中，甲医院每天根据病人 A 的观察记录生成病历然后上传到系统中，但是为了保护病人隐私以及搜索的方便，需要用访问结构与关键字加密后再上传到云系统中，从而只有用户属性满足访问结构的（如医生 B）才可以进行关键字搜索并获得相关信息。现实中可能会出现如下场景：医生 B 出差或外出度假，或者由于病人情况复杂医生 B 需要和乙医院的主任医生 C 进行共同会诊，即医生 C 希望能够在云系统中搜索到病人 A 的信息并查看，除此之外，这份共享的病历可能还需要将关键字更新。一个传统的方法就是由医生 B 将病人 A 的病历下载到本地解密后再用新的访问结构以及新的关键字加密后再上传到云系统中，这样医生 C 由于满足访问结构，从而可以从云系统中进行关键字搜索并获得信息。但是这种方法给医生 B 带来了额外的加密解密的负担，并且在这样一个大数据的时代，随

基金项目：中国国家自然科学基金资助项目（61572263，61502251，61502243）；江苏大学自然科学研究项目（14KJB520027，15KJB520027）；江苏省自然科学基金资助项目（BK20151511）；中国博士后科学基金资助项目（2015M581794）；江苏省博士后科学基金资助项目（1501023C）

作者简介：胡媛媛（1993-），女，硕士研究生，主要研究方向为信息安全（1054240974@qq.com）；陈燕俐（1969-），女，教授，硕导，博士，主要研究方向为计算机网络、信息安全；朱敏惠（1992-），女，硕士研究生，主要研究方向为信息安全.

ChinaXiv合作期刊
chinaXiv:201804.02035v1

着数据的增多，这样的搜索和共享的数量也会急剧增加。另外，将云系统中的密文下载到本地不仅给本地的存储和管理带来了压力，而且这也未能有效发挥云系统带来的存储优势。因此针对上述两个方面的问题，本文提出了满足实际应用需求的一个支持代理重加密的具有部分隐藏访问结构功能的基于属性密文可搜索方案，不仅实现了密文解密以及密文搜索功能的共享，还可支持关键字的更新。方案的访问结构采用的是 LSSS 线性秘密共享矩阵，不仅可支持细粒度的访问控制，且具有较高的计算效率。

1 相关介绍

2004 年，Boneh 等人[2]首次提出了公钥可搜索加密的概念，实现了用户无须对数据进行解密就能快速有效地进行搜索操作，以获得所需要的信息。随后，具有连接关键词[3]、模糊关键词[4]等功能的公钥可搜索加密方案也相继被提出。随着密码学的发展，学者们发现，虽然已有的公钥加密可搜索加密方案解决了对称可搜索加密中密钥传输的不确定性，但是在当前云存储快速发展，个人数据愈来愈多，这一复杂的分布式网络环境下，数据拥有者往往不能确切知道所有访问者的信息，但是又希望能给访问加密数据的用户加上一些限制条件，使得符合条件的用户才能搜索数据，其他人拒绝访问，通信模式不再是一对一的，显然传统的公钥可搜索加密[2]以及基于身份的可搜索加密技术[5]已经不能解决这一难题，为解决这个难题，基于属性的可搜索加密（ABKS）被提了出来。

2013 年，Wang 和 Kulvaibhavh 等人[6, 7]在传统的基于密文策略的属性加密方案[8]（CP-ABE）基础上提出了基于属性的密文检索方案（CP-ABKS）。2014 年，Zheng 等人[9]提出了一种可验证的基于 CP-ABE 的密文检索方案，该方案在加密过程中利用不同的访问结构加密不同的关键字，由服务器执行验证算法。验证过程中对于不同的访问结构产生不同的返回信息，用户根据返回的信息来判断服务器是否严格执行了验证算法。同年，李双等人[10]在密钥策略的属性加密方案（KP-ABE）基础上提出了 KP-ABE 的可搜索加密方案（KP-ABKS），该方案和文献[9]中一样都是采用效率较低的树型访问控制结构。此外，文献[10]中的方案在门限生成过程中包含了私钥，在门限上传到云服务器过程中，会产生用户私钥泄露的问题。随后一些支持用户属性撤销[11]，多用户[12]等特点的基于属性的可搜索加密方案被提出。上述可搜索加密方案由于访问结构会和关键字一起发送，而访问结构中通常包含一些敏感信息，所以存在用户隐私泄露的问题。尽管 Lai 等人[13]在 Waters 的 ABE[8]的基础上提出了隐藏访问结构的基于属性的加密方案，但是目前还没有人提出可隐藏访问结构的基于属性的可搜索加密方案，虽然 Mukti 等人[14]提出了隐藏访问结构的基于 CP-ABE 的可搜索加密方案，但是该方案是关键字等价于属性来生成门限，并不能实现真正的基于属性的密文可搜索。

尽管已经有大量关于基于属性的可搜索加密方案被提出，但是他们并不能满足实际应用中当授权用户不在线时将密文解密以及搜索权利授予给其他用户的需求。在 2014 年，Shao 等人[15]将传统的代理重加密[16]和可搜索加密[2]结合，提出了代理重加密的可搜索加密。随后一些支持代理重加密的可搜索加密方案[17, 18]也相继被提出，但是这些方案的通信模式都是一对一的，不能满足当前分布式网络环境的需求。所以 Shi 等人[19]将基于属性的加密可搜索加密与代理重加密的技术相结合提出支持关键字搜索的基于属性的代理重加密方案。但是该方案对关键字加密采用的是普通公钥加密技术，没有实现真正的一对多的通信模式，此外在查询门限和密文关键字比较过程中使用大量双线性配对运算而导致效率不高的问题。2015 年，Liang 等人[20]将 KP-ABKS 和代理重加密结合提出了可搜索的基于属性的代理重加密方案。但是该方案采用的是 KP-ABE，加密者不可以直接决定谁有权解密，只能为数据选择描述性的属性，只能相信密钥发布者，所以该方案并不能很好的控制访问策略，并且文献[19][20]均未能针对访问结构泄露敏感信息做处理。

本文贡献：针对目前基于属性的可搜索加密方案存在用户信息泄露以及不能实现密文解密以及搜索权限的代理、关键字更新等问题，提出了一个支持代理重加密的基于属性的密文检索方案（S-HABPRE-KU），不仅实现了密文的代理重加密，还可以支持关键字的更新。S-HABPRE-KU 方案主要的特点如下：

a)首次提出了一个符合实际应用需求的支持代理重加密的隐藏访问结构的基于属性的密文检索方案，实现了当授权用户不在线时将密文搜索和解密权限委托给其他用户，从而实现数据和密文的进一步安全有效的共享。

b)在密文进行重加密阶段，支持对关键字进行更新操作，以便在与他人共享密文之前，密文的关键字可以进一步更新。

c)方案采用了表达能力更强的 LSSS 访问结构，可以实现属性的与、或、非和陷门操作，细粒度地描述用户的属性，能够在可搜索加密的基础上提高效率，增加访问的灵活性，并减少存储代价。

d)方案采用部分隐藏访问结构的方式很好的保护用户的隐私，和文献[2]类似，方案中的属性由属性名和属性值两部分组成，但是和密文同时发送的访问结构只包含属性名，不包含具体属性值。

2 预备知识

2.1 双线性配对

设 G ，G_T 为两个阶为素数 p 的循环群，g 是 G 上的一个生成元。双线性映射 $e:G\times G\to G_T$ ，同时满足以下性质：

a）双线性。对于任意的 $a,b\in Z_p$ ，$g,g_1\in G$ ，都有 $e(g^a,g_1^b)=e(g,g_1)^{ab}$ 成立。

b）非退化性。存在 $g\in G$ ，使得 $e(g,g)\neq 1$ ，其中 1 代表 G_T 的单位元。

c）可计算性。对于 G 中的所有元素 g,g_1 ，存在一个有效算法能够计算出 $e(g,g_1)$ 。

chinaXiv:201804.02035v1

2.2 访问结构

设 $U=\{u_1,u_2,\cdots,u_n\}$ 是所有的属性集合，若存在访问结构 $A\subseteq 2^U$，如果对于任意的集合 B,C，有 $B\in A$，$B\subseteq C$，有 $C\in A$，那么称 A 是单调的。如果集合 A 是 2^U 的一个非空子集，那么称 A 是一个访问结构。包含在 A 中的集合称为授权集合，不包含在 A 中的集合称为非授权集合。

2.3 线性秘密共享方案(linear secret sharing scheme, LSSS)

一个定义在实体集 P 上的线性秘密共享方案 Π 是指：

a）所有实体的共享组成 Z_p 上的一个向量。

b）存在一个 $l\times n$ 的 Π 共享矩阵和一个从 $\{1,2,\cdots,l\}$ 到 P 的映射，随机选取一个向量 $v=(s,y_2,\cdots,y_n)\in Z_p$，其中 s 是要共享的秘密，那么 $M_i\cdot v$ 就是利用 Π 得到的关于 s 的 l 个共享值组成的向量，其中 $(Mv)_i$ 是属于实体 $\rho(i)$，记为 $\lambda_i=(M_i v^T)$。

按照以上定义的线性秘密共享方案 LSSS 都具有可重构的性质，假设 Π 是一个对应访问结构 A 的 LSSS，对于任何授权用户集 $S\in A$，定义 $I=\{i:\rho(i)\in S\}\subset\{1,2,\cdots,l\}$，如果 $\{\lambda_i\}$ 是秘密 s 根据 Π 的有效分享，那么存在一个常数集 $\{\omega_i\in Z_p\}_{i\in I}$ 使得 $\sum_{i\in I}\omega_i\lambda_i=s$；对于任何非授权用户集，存在向量 $\{\omega_i\in Z_p\}_{i\in I}$，使 $\omega_i M_i^T=0$。

2.4 判断性 q-BDHE(decisional q-parallel bilinear Diffie-Hellman exponent)假设

设存在一个阶为素数 p 的群 G，g 是 G 上的生成元，双线性映射：$e:G\times G\to G_T$，设 $\vec{y}=g,g^s,g^a,\cdots,\ g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}}$，$\forall_{1\le j\le q},g^{s\cdot b_j},g^{a/b_j},\cdots,g^{a^q/b_j},g^{a^{q+2}/b_j},\cdots,$，$g^{a^{2q}/b_j}$，$\forall_{1\le j,k\le q,k\ne j}\ g^{a\cdot s\cdot b_k/b_j},\cdots,g^{(a^q\cdot s\cdot b_k/b_j)}$，其中 $a,s,b_1,\cdots,b_q\in\mathbb{Z}_p$。将 $\vec{y}$ 交给敌手，不存在概率多项式时间算法 B，以不可忽略的优势将 $T=e(g,g)^{a^{q+1}s}\in G_T$ 与随机元素 $T\in G_T$ 区分。算法 B 的优势定义为

$$Adv_A^{D-q-parallelBDHE}=$$
$$|\Pr[B(\vec{y},T=e(g,g)^{a^{q+1}s})=0]-\Pr[B(\vec{y},T\in G_T)=0]|$$

2.5 判定性 DL(decisional linear assumption)假设

选择一个阶为素数 q 的群 G，挑战者从群 G 上选择生成元 g,f,h，随机值 $q_1,q_2\in Z_p$，敌手在获得 $Y=\{g,f,h,f^{q_1},g^{q_2}\}$ 以及随机值 $Q\in G$ 后，敌手必须将 $h^{q_1+q_2}\in G$ 与 G 中的随机值 Q 区分出来，定义输出 $b\in\{0,1\}$ 的算法解决判定 DL 的优势为 ε。若 $|Pr[\lambda(g,f,h,f^{q_1},g^{q_2},h^{q_1+q_2})=1]-Pr[\lambda(g,f,h,f^{q_1},g^{q_2},Q)=1]|\ge\varepsilon$ 成立，则说明敌手只能以优势 ε 攻破 DL 假设。

3 模型和攻击游戏

3.1 系统模型

本文构造的系统模型如图 1 所示，共包含三个实体，分别是授权中心，云服务器和云用户（包括数据属主和搜索用户）。其中授权中心负责初始化系统公钥、主密钥以及根据用户的属性集返回对应的私钥。数据属主选择需要上传的数据和文件后，为了保证数据和文件的安全性，必须加密后再上传。属主无须知道解密者的具体身份，只需要在加密时设置访问结构（如 PA）即可，为了防止访问结构中的敏感信息被泄露，本文采用部分隐藏访问结构。云服务器主要用来负责存储加密的数据，以及在用户上传搜索门限后进行搜索匹配算法，返回对应的搜索密文并解密得到共享数据和文件。此外，云服务器收到授权用户发送的重加密密钥（与另一个访问结构 PB，新的关键字 w’ 相关）后可以对原始密文进行重加密，充分发挥了云服务器的存储和计算能力。重加密后的密文可以由被授权用户进行搜索和解密操作，即使授权用户不在线的情况下仍然可以将搜索以及解密的权限委托给其他用户，实现了信息的安全有效共享。

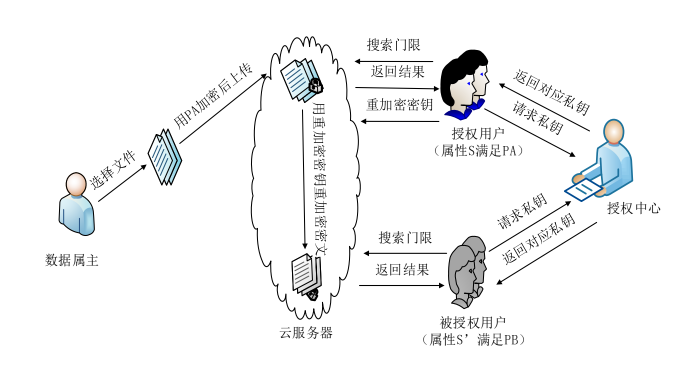


图 1 系统模型图

3.2 方案的一般模型

支持代理重加密的具有隐藏访问结构的功能的基于属性的密文可搜索方案包括以下 10 个算法：

a)系统初始化算法 $Setup(1^\kappa,U)$：输入安全参数 κ 和全局属性集合 U，输出系统公钥 PK 和主密钥 MSK。

b)私钥生成算法 $KeyGen(PK,MSK,Atts)$：输入系统公钥 PK、主密钥 MSK 和用户属性集 $Atts$，输出私钥 SK。

c)密文生成算法 $Enc(PK,(M,\rho,\Gamma),m,w)$：输入系统公钥 PK、访问结构 (M,ρ,Γ)，密文 m 和关键字 w，输出初始密文 CPH。

d)门限生成算法 $TokenGen(PK,SK,W)$：输入系统公钥 PK、用户私钥 SK 和待搜索关键字 W，输出门限 TK。这个门限是用来搜索与关键字 W 有关的加密数据。

e)密文搜索算法 $Search(PK,CPH,TK)$：输入系统公钥 PK、密文 CPH 和门限 TK，如果用户的属性满足密文中的访问结构且 w=W 就代表搜索成功，输出 1，否则输出 0。

f)解密算法 $Dec(PK,SK,CPH)$：输入系统公钥 PK、私钥 SK 和密文 CPH，由云服务器进行解密。

g)重加密密钥生成算法 $\mathrm{Re}KeyGen(PK,SK,(M',\rho',\Gamma'),KW)$：输入系统公钥 PK、用户私钥 SK 和新的访问结构 (M',ρ',Γ')，以及更新的关键字 KW，输出重加密密钥 RK，重加密密钥就是用来把基于访问结构 (M,ρ,Γ) 和关键字 w 的初始密文转换成相同明文下基于 (M',ρ',Γ') 和 KW 的重加密密文。

h)重加密密文生成算法 $\mathrm{Re}Enc(PK,CPH,RK)$：输入系统公钥 PK、初始密文 CPH 重加密密钥 RK，输出重加密密文 RCH。

i) 重加密密文搜索算法 $Rsearch(PK,TK,RCPH)$：输入系

ChinaXiv合作期刊

统公钥 PK、门限 TK 以及重加密密文 $RCPH$，如果用户的属性满足重加密密文中的访问结构且 $w=KW$ 就代表搜索成功，输出 1，否则输出 0。

j)重加密密文解密算 法 $Rdec(PK,SK,RCPH)$：输入系统公钥 PK、用户私钥 SK 和重加密密文 RCH，如果私钥中的属性集满足重加密密文中的访问结构那么即可成功解密，否则解密失败。

3.3 安全模型

S-HABPRE-KU 的安全目标是实现在随机预言模型下，假设没有一个概率多项式时间（PPT）的敌手能在一个不可忽视的优势下赢得下面这个选择明文攻击游戏和选择关键字攻击游戏，那么该方案是具有不可区分性抗选择访问结构的选择明文（IND-sAS-CPA）安全和抗选择关键字攻击（CKA）。选择明文攻击(CPA)是指攻击者可以获得公钥信息，并且可以根据自己的选择对不同的明文进行加密。关键字选择安全是指敌手在没有获得匹配的门限情况下，不能获得密文关键字以外的任何关键字信息。

以下是敌手和挑战者之间的选择明文攻击游戏，其中 C 是游戏的挑战者，κ 和 U 分别是安全参数和全局属性集。

1)选择明文攻击游戏：

a）攻击者初始化，敌手 A 宣布要挑战的访问结构 (M^*,ρ^*,Γ^*)。

b）系统初始化，挑战者 C 运行系统初始化算法 $Setup(1^\kappa,U)$，并将系统公钥 PK 发送给敌手 A。

c）第一阶段：敌手 A 可以访问以下预言机。

(a) $O_{SK}(Atts)$:敌手 A 选定属性集合 $Atts$，询问私钥 SK。挑战者 C 返回 $SK \leftarrow KeyGen(PK,MSK,Atts)$。

(b) $O_{TokenGen}(W,Atts)$:敌手 A 选定属性集合，关键字 W 询问门限值 TK。挑战者 C 返回 $TK \leftarrow TokenGen(PK,\ SK,W)$，其中 $SK \leftarrow KeyGen(PK,MSK,Atts)$。

(c) $O_{\mathrm{Re}\,KeyGen}(Atts,(M',\rho',\Gamma'),KW)$:敌手 A 给出属性集合 $Atts$，新的访问结构 (M',ρ',Γ')，一个关键字 KW，询问重加密密钥 $RK \leftarrow \mathrm{Re}\,KeyGen(PK,SK,(M',\rho',\Gamma'),KW)$。挑战者 C 返回 $RK \leftarrow \mathrm{Re}\,KeyGen(SK,(M',\rho',\Gamma'),KW)$ 给敌手 A，其中 $SK \leftarrow KeyGen(PK,MSK,Atts)$。

在该阶段，下述询问是被禁止的：

$O_{SK}(Atts)$ 时,任意的 $Atts$ 满足访问结构 (M^*,ρ^*,Γ^*)；

② $O_{\mathrm{Re}\,KeyGen}(Atts,(M',\rho',\Gamma'),KW)$ 时，任意的 $Atts$ 满足访问结构 (M^*,ρ^*,Γ^*)，并且 $O_{SK}(Atts)$ 时，任意的 $Atts$ 满足访问结构 (M^*,ρ^*,Γ^*)。

d）挑战：敌手 A 提交两个等长消息 m_0,m_1，挑战者 C 随机选其中之一 $m_{b\{b\in(0,1)\}}$ 和一个关键字 w^*，挑战者 C 将关键字密文 $CPH^*=Enc(PK,(M,\rho,\Gamma),m_b,w^*)_{\{b\in_R(0,1)\}}$ 发送给敌手 A。

e）第二阶段：此阶段敌手 A 重复第一阶段的操作。

f）猜测：敌手 A 输出猜测的值 b'。

如果 $b'=b$，敌手 A 获得胜利，敌手 A 获得胜利的优势定义为 $Adv_{S-HABPRE-KU}^{IND-sAS-CPA}(1^\kappa,U)=|pr[b'=b]-\frac{1}{2}|$。

定义 1 对于所有多项式时间的敌手 A，如果 $Adv_{S-HABPRE-KU}^{IND-sAS-CPA}$ 都是可以忽略不计的，那么 S-HABPRE-KU 方案在随机预言模型下是选择明文攻击安全的。

下面本文通过敌手模型形式化模拟的 CKA 安全定义，其中 I_{Enc} 表示与密文相关联的访问结构，I_{KeyGen} 表示与密钥相关的属性集合，函数 $F(I_{Enc},I_{KeyGen})=1$ 表示密钥中的属性集合满足密文中的访问结构，在系统建立之前由敌手决定要挑战的访问结构。

2)选择关键字攻击游戏：

系统建立：敌手选择一个要挑战的访问结构 I_{Enc}^*（I_{Enc}^* 不被一个不具备任何属性的用户所满足），将 I_{Enc}^* 发送给挑战者。挑战者执行初始化算法，产生系统公钥 PK 和系统主密钥 MSK。

阶段一：敌手可以在二项式时间内多次执行以下预言机，此外挑战者保存了一个初始状态为空的关键字链 L_{kw}。

a) $O_{KeyGen}(I_{KeyGen})$：如果 $F(I_{Enc}^*,I_{KeyGen})=1$，则系统终止运行。否则挑战者执行私钥生成算法 $KeyGen(I_{KeyGen})\rightarrow SK$ 并将对应的私钥 SK 返回给敌手。

b) $O_{TokenGen}(I_{KeyGen},w)$：敌手输入属性集合 I_{KeyGen} 和要查询的关键字 w。挑战者执行门限生成算法 $TokenGen(SK,w)\rightarrow TK$，并将门限值 TK 返回给敌手，其中 $SK \leftarrow KeyGen(I_{KeyGen})$。

挑战阶段：敌手选择关键字 w_0,w_1，$w_0,w_1\notin L_{kw}$。挑战者随机选择一个值 λ，其中 $\lambda\in\{0,1\}$，并计算密文 $cph^*=Enc(I_{Enc}^*,w_\lambda)$，挑战者将 cph^* 发给敌手。$w_0,w_1\notin L_{kw}$ 是为了防止敌手通过 $O_{TokenGen}(I_{KeyGen},w)$ 获取门限从而不断猜测 λ。

阶段二：敌手继续查询阶段一中的预言机，如果 $F(I_{Enc}^*,I_{KeyGen})=1$ 成立，则 (I_{KeyGen},w_0)，(I_{KeyGen},w_1) 不能作为 $O_{TokenGen}$ 的输入。

猜测：敌手输出 λ'。若 $\lambda'=\lambda$，则敌手赢得游戏，否则失败。

定义 2 若敌手在安全参数 κ 下以一个不可以忽略的优势赢得选择关键字攻击游戏，则本方案是安全的。

4 本方案描述

4.1 方案的具体实现

本方案主要包括十个算法：初始化，私钥生成，加密密文，产生门限，搜索匹配，解密密文，重加密密钥的生成，重加密密文的生成，重加密密文的搜索匹配以及密文重解密算法，下面进行详细描述。

a) $Setup(1^\kappa,U)\rightarrow\{\mathrm{PK,MSK}\}$。

输入安全参数 κ 和全局属性集合 U，$|U|=n$，授权中心执行初始化算法。首先选择两个阶为素数 p 的循环群 G,G_T，随机选择生成元 $g,g_1\in G$，再取三个随机数 $a,b,c\in Z_p$，接着选择随机值 $u_1,\cdots,u_n\in G$，哈希函数 $H_1:\{0,1\}^*\rightarrow Z_p$，$H_2:\{0,1\}^*\rightarrow Z_p$。输出公共参数 $\mathrm{PK}=\{g_1,g^a,g^b,g^c,e(g,g)^{bc},u_1,\cdots,u_n\}$，授权中心保存系统主密钥 $MSK=\{a,b,c\}$。

chinaXiv:201804.02035v1

chinaXiv:201804.02035v1

b) $KeyGen(PK, MSK, Atts) \rightarrow SK$。

输入系统公钥 PK 和主密钥 MSK 以及用户属性集 $Atts$，授权中心执行密钥生成算法。选取随机值 $t \leftarrow Z_p$，计算 $K = g^{bc+at}$，$L = g^t$，对于随机选择 $s_i \leftarrow Z_p$，$\forall s_i \in Atts$，$K_i = (u_i^{s_i})^t$。输出用户私钥 $SK = \{K, L, \{K_i\}_{s_i \in Atts}\}$。

c) $Enc(PK, m, (M, \rho, \Gamma), w) \rightarrow CPH$。

输入加密的消息 m、访问结构 (M, ρ, Γ) 和需要加密的关键字 w，数据拥有者执行加密算法。其中，M 是 $l \times n$ 的线性矩阵，ρ 是一个单映射函数，可以将矩阵的每一行映射成用户属性，$\Gamma = (t_{\rho(1)}, \cdots, t_{\rho(l)}) \in Z_p^l$，从第 1 行到第 l 行，计算 $\lambda_i \leftarrow \vec{v} \cdot M_i$，其中 M_i 是矩阵 M 第 i 行对应的向量。首先选择两个随机值 $q_1, q_2 \leftarrow Z_p$，然后选择一组随机值构成随机向量 $\vec{v} = (q_2, y_2, \cdots, y_n) \in Z_p$，其中 q_2 是共享的秘密，再选择随机值 $r_1, \cdots, r_l \leftarrow Z_p$。计算密文如下：$A = me(g,g)^{bcq_2}$，$B = g^{q_2}$，$B_1 = g_1^{q_2}$，$C_x = g^{a\lambda_x}(u_{\rho(x)}^{t_{\rho(x)}})^{-r_x}$，$D_x = g^{r_x}$，$W_1 = g^{cq_1}$，$W_2 = g^{b(q_1+q_2)} g^{aH_1(w)q_1}$。输出密文 $CPH = \{A, B, B_1, \forall x \in [1,l]\{C_x, D_x\}, W_1, W_2\}$。

d) $TokenGen(PK, SK, W) \rightarrow TK$。

输入用户私钥 SK 和待查的关键字 W，云服务器执行门限生成算法。选择随机值 $\sigma \leftarrow Z_p$，$T_1 = (g^b g^{aH_1(W)})^{\sigma}$，$T_2 = g^{\sigma c}$，$T_3 = K^{\sigma} = g^{(bc+at)\sigma}$，$T_4 = L^{\sigma} = g^{t\sigma}$，$\forall x \in Atts$，$T_x = (K_x)^{\sigma} = (u_x^{s_x})^{t\sigma}$。输出门限 $TK = \{T_1, T_2, T_3, T_4, T_x\}_{s_x \in Atts}$。

e) $Search(PK, TK, CPH) \rightarrow 0/1$。

输入门限 TK 和密文 CPH，云服务器执行密文检索算法。假设用户的属性集 $Atts$ 满足访问结构 (M, ρ)，则一定存在一组值 $\{\omega_i \in Z_p\}_{i \in I}$ 使得 $\sum_{i \in I} \omega_i \lambda_i = q_2$，其中 $I \subset \{1, \cdots, l\}, I = \{i, \rho(i) \in Atts\}$。计算过程如下 $Eroot = \prod_{i \in I} (e(C_i, T_4) e(D_i, T_{\rho(i)}))^{\omega_i}$，$E_1 = e(W_2, T_2) \cdot Eroot$，$E_2 = e(W_1, T_1) e(T_3, B)$。如果 $E_1 = E_2$ 则输出 1,代表搜索成功,否则输出 0。

f) $Dec(PK, SK, CPH) \rightarrow m/\perp$。

输入私钥 SK 和密文 CPH，云服务器执行解密算法。对于原始密文，如果关键搜索成功，则代表存在相关密文，并且用户的私钥中的属性已经满足密文中的访问结构，即已经找到这样一组值 $\{\omega_i \in Z_p\}_{i \in I}$ 使得 $\sum_{i \in I} \omega_i \lambda_i = q_2$ 成立，然后即可成功解密密文。即先计算 $Z = \frac{e(B, K)}{\prod_{i \in I} \left(e(C_i, L) e(D_i, K_i)\right)^{\omega_i}}$，然后 $A / Z = m$ 得到消息 m。否则解密失败输出 $\perp$。

g） $\mathrm{Re}KeyGen(PK, SK, (M', \rho', \Gamma'), KW) \rightarrow RK$。

输入系统公钥 PK、授权用户私钥 SK、新的访问结构 (M', ρ', Γ')，新的关键字 KW，授权用户执行重加密密钥生成算法。选择随机值 q_2' 和随机矢量 $v' = (q_2', y_2', \cdots, y_n')$，$y_2', \cdots, y_n' \in Z_p$，再随机选择 $\delta \in \{0,1\}^*$，其中，M' 是 $l \times n$ 的线性矩阵，ρ' 是一个单映射函数，可以将矩阵的每一行映射成用户属性名，$\Gamma = (t'_{\rho'(1)}, \cdots t'_{\rho'(l)}) \in Z_p^l$ 是对应的属性值，从第 1 行到第 l 行，计算 $\lambda_i' \leftarrow \vec{v}' \cdot M_i'$，其中 M_i' 是矩阵 M' 第 i 行对应的向量。然后随机选择 $r_1', \cdots, r_l' \leftarrow Z_p$。计算重加密密文如下：$rk_1 = \delta e(g,g)^{bcq_2'}$，$rk_2 = g^{q_2'}$，$rk_3 = g^{b(q_1'+q_2')} g^{aH_1(KW)q_1'}$，$rk_4 = g^{cq_1'}$，$rk_{5,i} = g^{a\lambda_i'}(u_{\rho'(i)}^{t'_{\rho'(i)}})^{-r_i'}$，$rk_{6,i} = g^{r_i'}$，随机选择 $\theta \in Z_p$，$rk_7 = (K)^{H_2(\delta)} g_1^{\theta} = (g^{bc+at})^{H_2(\delta)} g_1^{\theta}$，$rk_8 = g^{\theta}$，$rk_9 = L^{H_2(\delta)} = (g^t)^{H_2(\delta)}$，$R_i = K_i^{H_2(\delta)} = \left((u_i^{s_i})^t\right)^{H_2(\delta)}$，输出重加密密钥 $RK = \{rk_1, rk_2, rk_3, rk_4, rk_{5,i}, rk_{6,i}, rk_7, rk_8, rk_9, R_i\}_{1 \le i \le l'}$。

h） $\mathrm{Re}Enc(PK, CPH, RK) \rightarrow RCPH$。

输入原始密文 CPH 和重加密密钥 RK，云服务器运行重加密算法。若 $I \subset \{1, \cdots, l\}, I = \{i, \rho(i) \in Atts\}$，在属性满足访问结构时，存在一个常数集 $\{\omega_i \in Z_p\}_{i \in I}$，使得 $\sum_{i \in I} \lambda_i \omega_i = q_2$，然后计算 $rc = \frac{e(B, rk_7) / e(B_1, rk_8)}{\prod_{i \in I} \left(e(C_i, rk_9) e(D_i, R_i)\right)^{\omega_i}}$，最后输出重加密密文 $RCPH(rk_1, rk_2, rk_3, rk_4, rk_{5,i}, rk_{6,i}, rc)$。

i） $Rsearch(PK, TK, RCPH) \rightarrow 0/1$。

输入门限 TK 和重加密密文 CPH，云服务器执行密文检索算法。假设用户的属性集 $Atts'$ 满足访问结构 (M', ρ', Γ')，则一定存在一组值 $\{\omega_i' \in Z_p\}_{i \in I}$ 使得 $\sum_{i \in I} \omega_i' \lambda_i' = q_2'$，其中 $I \subset \{1, \cdots, l\}, I = \{i, \rho(i) \in Atts\}$。计算过程如下 $Eroot' = \prod_{i \in I} (e(rk_{5,i}, T_4) e(rk_{6,i}, T'_{\rho(i)}))^{\omega_i'}$，$E_1' = e(rk_3, T_2) \cdot Eroot'$，$E_2' = e(rk_4, T_1) e(T_3, rk_2)$，如果 $E_1 = E_2$ 则输出 1，代表搜索成功，否则输出 0。

j） $Rdec(PK, SK, RCPH) \rightarrow m/\perp$。

输入被授权人的私钥 SK 和重加密密文 $RCPH$。当用户属性集 $Atts'$ 不满足访问结构 (M', ρ') 时,输出 $\perp$，否则根据私钥和重加密密文恢复出 δ，$rk_1 / Z' = \delta$，其中 $Z' = \frac{e(rk_2, K)}{\prod_{i \in I} \left(e(rk_{5,i}, L) e(rk_{6,i}, K_i)\right)^{\omega_i}}$，然后其中解密密文 $m = A / rc^{\frac{1}{H_2(\delta)}}$。

4.2 正确性验证

本方案正确性可按如下方式进行验证。

a）第 e)步搜索验证算法的正确性如下：

chinaXiv:201804.02035v1

$$Eroot=\prod_{i\in I}(e(C_i,T_4)e(D_i,T_{\rho(i)}))^{\omega_i}$$
$$=\prod_{i\in I}\left(e(g^{a\lambda_i}\left(u_{\rho(i)}^{t_{\rho(i)}}\right)^{-r_i},g^{t\sigma})e(g^{r_i},(u_i^{s_i})^{t\sigma}\right)^{\omega_i}$$
$$=\prod_{i\in I}\left(e(g^{a\lambda_i},g^{t\sigma})e(\left(u_{\rho(i)}^{t_{\rho(i)}}\right)^{-r_i},g^{t\sigma})e(g^{r_i},(u_i^{s_i})^{t\sigma}\right)^{\omega_i}$$
$$=\prod_{i\in I}\left(e(g^{a\lambda_i},g^{t\sigma})\right)^{\omega_i}$$
$$=e(g,g)^{at\sigma q_2}$$

$$E_1=e(W_2,T_2)\cdot Eroot$$
$$=e(g^{b(q_1+q_2)}g^{aH_1(w)q_1},g^{\sigma c})e(g,g)^{at\sigma q_2}$$
$$=e(g^{b(q_1+q_2)},g^{\sigma c})e(g^{aH(w)q_1},g^{\sigma c})e(g,g)^{at\sigma q_2}$$
$$=e(g,g)^{b\sigma c(q_1+q_2)}e(g,g)^{a\sigma c q_1 H(w)}e(g,g)^{at\sigma q_2}$$

$$E_2=e(W_1,T_1)e(T_3,B)$$
$$=e(g^{cq_1},(g^b g^{aH_1(W)})^{\sigma})e(g^{cb\sigma}g^{at\sigma},g^{q_2})$$
$$=e(g^{cq_1},g^{b\sigma})e(g^{cq_1},g^{aH(W)\sigma})e(g^{cb\sigma},g^{q_2})e(g^{at\sigma},g^{q_2})$$
$$=e(g,g)^{cb\sigma(q_1+q_2)}e(g,g)^{ca\sigma q_1 H(W)}e(g,g)^{at\sigma q_2}$$

由上式可知，当且仅当 $w=W$，即密文中的关键字和门限中的关键字相同时 $E_1=E_2$ 成立。

b）第 f)步解密算法正确性验证如下：

$$Z=\frac{e(B,K)}{\prod_{i\in I}\left(e(C_i,L)e(D_i,K_i)\right)^{\omega_i}}$$
$$=\frac{e(g^{q_2},g^{bc+at})}{\prod_{i\in I}\left(e(g^{a\lambda_i}(u_{\rho(i)}^{t_{\rho(i)}})^{-r_i},g^t)e(g^{r_i},(u_i^{s_i})^t)\right)^{\omega_i}}$$
$$=\frac{e(g^{q_2},g^{bc})e(g^{q_2},g^{at})}{\prod_{i\in I}\left(e(g^{a\lambda_i},g^t)e((u_{\rho(i)}^{t_{\rho(i)}})^{-r_i},g^t)e(g^{r_i},(u_i^{s_i})^t)\right)^{\omega_i}}$$
$$=e(g^{q_2},g^{bc})$$

$$A/Z=me(g,g)^{bcq_2}\ /\ e(g,g)^{bcq_2}=m$$

c）第 h)步重加密密文算法中的 rc 计算如下:

$$rc=\frac{e(B,rk_7)/e(B_1,rk_8)}{\prod_{i\in I}\left(e(C_i,rk_9)e(D_i,R_i)\right)^{\omega_i}}$$
$$=\frac{e(g^{q_2},(g^{bc+at})^{H_2(\delta)}g_1^{\theta})/e(g_1^{q_2},g^{\theta})}{\prod_{i\in I}\left(e(g^{a\lambda_i}(u_{\rho(i)}^{t_{\rho(i)}})^{-r_i},(g^t)^{H_2(\delta)})e(g^{r_i},\left((u_i^{s_i})^t\right)^{H_2(\delta)})\right)^{\omega_i}}$$
$$=\frac{e(g^{q_2},(g^{bc+at})^{H_2(\delta)})}{\prod_{i\in I}\left(e(g^{a\lambda_i},(g^t)^{H_2(\delta)})e((u_{\rho(i)}^{t_{\rho(i)}})^{-r_i},(g^t)^{H_2(\delta)})e(g^{r_i},\left((u_i^{s_i})^t\right)^{H_2(\delta)})\right)^{\omega_i}}$$
$$=\frac{e(g^{q_2},g^{at})^{H_2(\delta)}e(g^{q_2},g^{bc})^{H_2(\delta)}}{\prod_{i\in I}\left(e(g^{a\lambda_i},(g^t)^{H_2(\delta)})\right)^{\omega_i}}$$
$$=e(g^{q_2},g^{bc})^{H_2(\delta)}$$

d）第 i)步重加密密文的搜索验证算法正确性如下：

$$Eroot'=\prod_{i\in I}(e(rk_{5,i},T_4)e(rk_{6,i},T_{\rho(i)}))^{\omega_i'}$$
$$=\prod_{i\in I}\left(e(g^{a\lambda_i'}\left(u_{\rho'(i)}^{t'_{\rho'(i)}}\right)^{-r_i'},g^{t\sigma})e(g^{r_i'},(u_i^{s_i})^{t\sigma}\right)^{\omega_i'}$$
$$=\prod_{i\in I}\left(e(g^{a\lambda_i'},g^{t\sigma})e(\left(u_{\rho'(i)}^{t'_{\rho'(i)}}\right)^{-r_i'},g^{t\sigma})e(g^{r_i'},(u_i^{s_i})^{t\sigma}\right)^{\omega_i'}$$
$$=\prod_{i\in I}\left(e(g^{a\lambda_i'},g^{t\sigma})\right)^{\omega_i'}$$
$$=e(g,g)^{at\sigma q_2'}$$

$$E_1'=e(rk_3,T_2)\cdot Eroot'$$
$$=e(g^{b(q_1'+q_2')}g^{aH_1(KW)q_1'},g^{\sigma c})e(g,g)^{at\sigma q_2'}$$
$$=e(g^{b(q_1'+q_2')},g^{\sigma c})e(g^{aH(KW)q_1'},g^{\sigma c})e(g,g)^{at\sigma q_2'}$$
$$=e(g,g)^{b\sigma c(q_1'+q_2')}e(g,g)^{a\sigma c q_1' H(KW)}e(g,g)^{at\sigma q_2'}$$

$$E_2=e(rk_4,T_1)e(T_3,rk_2)$$
$$=e(g^{cq_1'},(g^b g^{aH_1(W)})^{\sigma})e(g^{cb\sigma}g^{at\sigma},g^{q_2'})$$
$$=e(g^{cq_1'},g^{b\sigma})e(g^{cq_1'},g^{aH(W)\sigma})e(g^{cb\sigma},g^{q_2'})e(g^{at\sigma},g^{q_2'})$$
$$=e(g,g)^{cb\sigma(q_1'+q_2')}e(g,g)^{ca\sigma q_1' H(W)}e(g,g)^{at\sigma q_2'}$$

由上式可知，当且仅当 $KW=W$，即重加密密文中的关键字和门限中的关键字相同时，$E_1'=E_2'$ 成立。

e）第 j)步重解密算法的正确性验证如下：

$$Z'=\frac{e(rk_2,K)}{\prod_{i\in I}\left(e(rk_{5,i},L)e(rk_{6,i},K_i)\right)^{\omega_i}}$$
$$=\frac{e(g^{q_2'},g^{bc+at})}{\prod_{i\in I}\left(e(g^{a\lambda_i'}(u_{\rho'(i)}^{t'_{\rho(i)}})^{-r_i'},g^t)e(g^{r_i'},(u_i^{s_i})^t)\right)^{\omega_i}}$$
$$=\frac{e(g^{q_2'},g^{bc})e(g^{q_2'},g^{at})}{\prod_{i\in I}\left(e(g^{a\lambda_i'},g^t)e((u_{\rho'(i)}^{t'_{\rho(i)}})^{-r_i'},g^t)e(g^{r_i'},(u_i^{s_i})^t)\right)^{\omega_i}}$$
$$=e(g^{q_2'},g^{bc})$$

$$rk_1/Z'=\delta e(g,g)^{bcq_2'}\ /\ e(g,g)^{bcq_2'}=\delta$$

$$A/rc^{\frac{1}{H_2(\delta)}}=me(g,g)^{bcq_2}\ /\ e(g^{q_2},g^{bc})=m$$

由上式可知，当且仅当能够找到 $\{\omega_{\rm i}\in Z_p\}_{i\in I}$ 这样一组向量使得 $\prod_{i\in I}\lambda_i'\omega_i=q_2'$ 时，才可以得到消息 m。

5 安全性分析与证明

安全的可搜索加密要求云服务器不能获得关于明文的任何信息，本文的密文包括消息部分以及关键字部分，所以下面证明了本方案对于密文的选择明文攻击的安全性以及选择关键字攻击的安全性。

定理 1 假设 q-BDHE 问题是难解的，则本方案在随机预言模型下是 IND-sAS-CPA 安全。

证明 假设在游戏中存在一个多项式时间的敌手，能以 $\varepsilon=Adv_A$ 的优势赢得本方案，则可构造一个挑战者 C 进行判定性 q-parallel BDHE 假设，从而判断 $T=e(g,g)^{a^{q+1}\cdot s}$ 还是 $T\in G_T$。挑战者 C 和敌手 A 进行如下选择明文攻击游戏：

挑战者 C 输入 (p,g,G,G_T,e)，q-parallel BDHE 的实例 $\vec{y},T$。

攻击者初始化：首先敌手 A 向挑战者 C 宣布要挑战的目标访问结构 (M^*,ρ^*,Γ^*)，其中 M^* 是一个 $l^*\times n^*$ 大小的矩阵，l^* 是行数，n^* 是列数，$l^*,n^*\le q$，$\Gamma^*=(t^*_{\rho(1)},\cdots,t^*_{\rho(l)})\in Z_p^l$，其中 $\rho(i)$ 对应属性名，$t^*_{\rho(i)}$ 对应属性值。

系统初始化：挑战者 C 选取阶为素数 p，g,g_1 为的群 G 上的生成元。随机选取 $\alpha',a\in Z_p^*$，令 $bc=\alpha'+a^{q+1}$，则 $e(g,g)^{bc}=e(g^a,g^{a^q})e(g,g)^{\alpha'}$。挑战者 C 返回系统公钥 pub={$g^a,e(g,g)^{bc}$} 和系统主密钥 msk={a,b,c}，其中挑战者 C

chinaXiv:201804.02035v1

对私钥不可知。下面介绍如何通过建立表 $H_j^{list}(j\in\{1,2\})$ 来模拟执行随机预言 $H_j(j\in\{1,2\})$。敌手 A 可以在任何时候进行适应性的询问随机预言 $H_j(j\in\{1,2\})$，H_j 由挑战者 C 控制，挑战者 C 持有 $H_j^{list}(j\in\{1,2\})$ 列表，列表起初为空，挑战者 C 按如下回答询问。

（a）$H_1(kw)$：如果查询的关键字 kw 在随机预言机 H_1^{list} 在表中已存在 (kw,κ_1)，则返回已有值 κ_1，这里 $\kappa_1\in Z_p^*$；否则，挑战者 C 设置 $H_1(kw)=\kappa_1$，将 (kw,κ_1) 添加到 H_1^{list} 中，并返回 $H_1(kw)=\kappa_1$ 给敌手 A。

（b）$H_2(\delta)$：如果查询的 δ 在随机预言机 H_2^{list} 在表中已存在 (δ,κ_2)，则返回已有值 κ_2，这里 $\kappa_2\in Z_p^*$；否则，挑战者 C 设置 $H_2(\delta)=\kappa_2$，将 (δ,κ_2) 添加到 H_2^{list} 中，并返回 $H_2(\delta)=\kappa_2$ 给敌手 A。

阶段 1　敌手 A 进行一系列查询，挑战者 C 按如下进行回答。

(a) $O_{SK}(Atts)$：敌手 A 按如下为属性集 $Atts$ 构造私钥。如果 $Atts$ 满足目标访问结构 (M^*,ρ^*,Γ^*)，则挑战者 C 返回 $\perp$，如果在 SK^{list} 中 $(SK,Atts,*)$ 记录存在，则返回对应值 SK；如果 $Atts$ 不满足目标访问结构 (M^*,ρ^*,Γ^*)，则挑战者 C 响应敌手的私钥请求。首先随机选取 $r\in Z_p^*$，由 LSSS 的重构特性知，存在一个常数向量 $\vec{\omega}=(\omega_1,\ldots,\omega_{n^*})\in Z_p^*$，其中 $\omega_1=-1$。如果 $\forall i,\rho^*(i)\in Atts$，则有 $\vec{\omega}\cdot M_i^*=0$。

令 $t=r+\omega_1a^q+\omega_2a^{q-1}+\ldots+\omega_{n^*}a^{q-n^*+1}$，则 $L=g^r\prod_{i=1,\ldots,n^*}(g^{a^{q+1-i}})^{\omega_i}=g^t$，$K=g^{\alpha'}g^{ar}\prod_{i=2,\ldots,n^*}(g^{a^{q+2-i}})^{\omega_i}$。对于集合 $Atts$ 中任意元素 s_i 存在 $K_i=(u_i^{s_i})^t$。将 $(Atts,SK)$ 添加到 SK^{list} 中，并返回私钥 SK 给敌手 A。

(b)用一个属性集 S 和访问结构 (M',ρ',Γ') 来访问重加密密钥。如果在 rk^{list} 中 $(S,(M',\rho',\Gamma'),kw,rk_{s'\to(M',\rho',\Gamma')})$ 记录已存在，挑战者 C 返回重加密密钥 RK。否则,如果属性集 $Atts$ 满足访问结构 (M^*,ρ^*,Γ^*)，挑战者 C 返回 $\perp$ 给敌手 A 并终止游戏。如果属性集 $Atts$ 不满足访问结构 (M^*,ρ^*,Γ^*)，挑战者 C 先运行 $O_{SK}(Atts)$ 产生私钥 SK，然后再按如下输出重加密密钥 RK。挑战者 C 随机选择 $\theta\in Z_p,r_1',\cdots,r_l'\in Z_p$，计算重加密密钥 $rk_7=(K)^{H_2(\delta)}g_1^{\theta}=(g^{bc+at})^{H_2(\delta)}g_1^{\theta}$，$rk_8=g^{\theta}$，$rk_9=L^{H_2(\delta)}=(g^t)^{H_2(\delta)}$，$R_i=K_i^{H_2(\delta)}=\left((u_i^{s_i})^t\right)^{H_2(\delta)}$。最后，挑战者 C 返回 RK 给敌手。最后模拟者将 $(Atts,SK)$ 和 $(Atts,(M',\rho'),kw',RK)$ 分别加入私钥列表 SK^{list} 和重加密密钥列表 rk^{list}。

挑战：敌手 A 向挑战者 C 提交两个长度相同的密文 (m_0,m_1)，挑战者 C 随机选取 $b\in\{0,1\}$，加密消息 m_b，并按如下进行回答。对于 M^* 的每一行 i，设置 $s_i=\rho^*(i)$，随机选取 $\vec{v}=(q_2,q_2\cdot a+y_2',q_2\cdot a^2+y_3',\cdots,q_2\cdot a^{n-1}+y_n'\in Z_p)$，然后选择 $r_1',\cdots,r_l'\in Z_p$，向量 $\vec{v}$ 用来分享秘密 q_2，对于所有的 $i\in\{1,\cdots,l^*\}$，R_i 表示所有的 $i\neq k$，但 $\rho^*(i)=\rho^*(k)$ 的集合。然后计算挑战者选择 $A^*\in\{0,1\}^{2k}$ 隐含定义 $T\cdot e(g^{q_2},g^{a'})=A^*/m_b$，并设置 $B^*=g^{q_2}$ 和 $B_1^*=g_1^{q_2}$，对于 $i=1,\cdots,n^*$，$C_i^*=(u_{\rho(i)}^{t_{\rho(i)}})^{-r_i'}(\prod_{j=2,\ldots,n^*}(g^a)^{M_{i,j}^*y_i'})g^{b_i\cdot q_2\cdot(-z_{x^*})}\cdot\prod_{k\in R_i}\prod_{j=1,\cdots,n^*}(g^{a^jq_2(b_i/b_k)})^{M_{k,j}^*})^{-1}$，$D_i^*=g^{r_i'+sb_i}$，因此创建密文 $CT^*=(A^*,B^*,B_1^*,C_i^*,D_i^*)_{1\le i\le n}$。若 $T=e(g,g)^{a^{q+1}s}$，那么 CT^* 是一个有效的密文。

阶段 2　像阶段一中的一样进行预言机询问。

猜测：敌手 A 给出猜测 $b'\in\{0,1\}$，当 $b=b'$ 时，挑战者 C 输出 1，也就是 $T=e(g,g)^{a^{q+1}s}$。否则挑战者 C 输出 0，也就是 T 为 G_T 上的随机元素。下面计算挑战者 C 成功的概率。

当输出为 1 时，即 $T=e(g,g)^{a^{q+1}s}$ 时，也就是敌手得到的是关于 m_b 的有效密文，模拟是完美的。通过定义，本文知道敌手 A 能正确猜测结果具有不可忽视的优势 ε，因此概率为 $\Pr\left[b'\neq b\,|\left(\vec{y},T=e(g,g)^{a^{q+1}s}\right)=0\right]=\frac{1}{2}+Adv_A$。

当输出为 0 时，即 T 是 G_T 上的一个随机数，敌手获取不到任何关于密文的信息，因此，猜测正确率为 $\Pr\left[b'\neq b\,|\left(\vec{y},T\in G_T\right)=0\right]=\frac{1}{2}$。

这样，挑战者 C 在判定性 q-parallel BDHE 游戏中就有不可忽略的优势 $\frac{\varepsilon}{2}$。

定理 2　假设该方案在随机预言模型下是 sAS-CPA 安全的，那么该方案是选择可抵抗同谋攻击的。

证明　在 IND-sAS-CPA 游戏中，敌手 A 能从 O_{rk} 中获得 $RK_{Atts\to(M',\rho')}$ 和 $RK_{Atts''\to(M'',\rho'')}$，这里分别需要 $Atts\models(M^*,\rho^*)$ 和 $Atts'\models(M'',\rho'')$。因为游戏中定义的限制，敌手 A 不能询问任意 $Atts'\models(M',\rho')$ 的私钥 SK（敌手 A 也不能询问 $Atts\models(M^*,\rho^*)$ 的私钥 SK），但是可以询问任意的 $Atts''\models(M'',\rho'')$ 的私钥 $SK_{Atts''}$。

假设 sAS-CPA 安全的方案是不能抵抗选择同谋攻击的。那么敌手 A 能从 $rk_{Atts'\to(M'',\rho'')}$ 中通过同谋获得 SK。使用 $rk_{Atts\to(M',\rho')}$，敌手 A 能重加密挑战密文 CPH，然后，敌手 A 用 SK 解密重加密密文，以便输出 b 的值，这个就与 sAS-CPA 安全的定义矛盾。所以该假设不成立，证明完毕。

定理 3　若在通用模型下 DL 假设成立，则不存在多项式时间敌手以不可忽略的优势区分选择关键字攻击游戏。

证明　在选择关键字攻击游戏中敌手尝试区分 $g^{b(q_1+q_2)}g^{aH_1(w_1)q_1}$，$g^{b(q_1+q_2)}g^{aH_1(w_0)q_1}$。挑战者随机选择 $\Theta\in Z_p$，$g^{\Theta}\in G$，如果敌手赢得选择关键字攻击游戏的优势为 ε，则敌

chinaXiv:201804.02035v1

手存在 $\frac{\varepsilon}{2}$ 的概率区分 g^{Θ} 和 $g^{a(t_1+t_2)+t_1H_1(w)}$ 。

系统建立：挑战者建立系统，对于属性有 $\forall Atts_x \in [1,|U|]$，挑战者选择生成元 $g \in G$，然后选择 $u_x \in G$， $a,b,c \in Z_p$，将参数 $\{g^a, g^b, g^c, u_1, \cdots, u_n\}$ 发送给敌手。敌手选择一个要挑战的访问结构 (M,ρ) 发送给挑战者。

阶段 1 ：敌手可以在任意多项式时间内多次查询以下预言机。

a) $O_{KeyGen}(Atts)$：敌手输入属性集，挑战者执行密钥生成算法，随机选择 $t \in Z_p$，计算 $K = g^{ac}g^{bt}$， $L = g^t$， $K_i = (u_i^{s_i})^t$，$\forall s_i \in Atts$ 。挑战者将 $\{Atts, K, L, \{K_i\}_{\forall s_i \in Atts}\}$ 返回给敌手。

b) $O_{Token}(Atts, w)$：挑战者先查询预言机 O_{KeyGen} 生成私钥 $SK = \{Atts, K, L, \{K_i\}_{s_i \in Atts}\}$，然后选择随机值 $\sigma \in Z_p$，之后计算 $T_1 = (g^b g^{aH(W)})^{\sigma}$， $T_2 = g^{\sigma c}$， $T_3 = K^{\sigma} = g^{bc\sigma}g^{at\sigma}$， $T_4 = L^{\sigma} = g^{t\sigma}$，$\forall x \in Atts$ $T_x = (K_x)^{\sigma} = (u_x^{s_x})^{t\sigma}$ ，然后将门限值 $TK = \{T_1, T_2, T_3, T_4, T_x\}$ 传给敌手，如果属性集合满足访问结构，那么就将关键字 w 加入 L_{kw} 。

挑战阶段：敌手给出两个等长的关键字 $w_0, w_1 \notin L_{kw}$，挑战者产生两个随机值 $q_1, q_2 \in Z_p$，利用线性共享矩阵共享秘密 q_2。挑战者随机选择 $\lambda \in \{0,1\}$，若 $\lambda = 0$，挑战者随机选择 $\Theta \in Z_p$，计算 $W_1 = g^{cq_1}$，$W_2 = g^{\Theta}$，$W_3 = g^{q_2}$，$C_x = g^{a\lambda_x}(u_{\rho(x)}^{t_{\rho(x)}})^{-r_x}$，$D_x = g^{r_x}$，否则计算 $g^{a(t_1+t_2)+t_1H_1(w)}$ 。

阶段 2 若敌手能够从预言机的输出中构造出 $e(g,g)^{\Theta a(q_1+q_2)}$，则敌手可以区分 g^{Θ}， $g^{a(q_1+q_2)}$ 。因此本文需要证明敌手只能以可忽略的优势构造出 $e(g,g)^{\Theta a(q_1+q_2)}$，即敌手只能以可以忽略的优势赢得选择关键字攻击游戏。

在通用模型中 φ_0, φ_1 是从 Z_p 到一个元素个数为集合 p^3 的内射函数，敌手只能以可以忽略的概率从 φ_0, φ_1 的映射中猜中元素。因此本文考虑敌手从预言机输出中构造 $e(g,g)^{\delta a(q_1+q_2)}$ 的概率。

考虑对一些 g^{δ} 如何构造 $e(g,g)^{\delta a(q_1+q_2)}$，$q_1$ 只在 cq_1 中出现，为了构造 $e(g,g)^{\delta a(q_1+q_2)}$，$\delta$ 需要包含 c 。设 $\delta = \delta' c$，这样敌手为了构造 $e(g,g)^{\delta a(q_1+q_2)}$，敌手为了构造 $e(g,g)^{\delta a(q_1+q_2)}$ 需要构造 $\delta' acq_2$ 。这将要使用到 q_2，$ac+bt$，因为 $q_2(ac+bt) = acq_2 + btq_2$。敌手需要消去 btq_2，为了消去 btq_2，需要使用 λ_i， r_i， t， λ_i 是根据访问结构 (M,ρ) 共享 q_2。但是根据这些元组不可能构造出 btq_2，因为当且仅当密钥中的属性集合满足密文中的访问结构才可以被重构。

因此本文可以得出结论，敌手只能以一个可以忽略的优势赢得改进的选择关键字攻击游戏，证明结束。

6 性能分析

本文主要从计算开销和通信开销两个方面与密文可搜索方案 Wang[6]和方案 Zheng[8]的进行了比较与分析。

首先将方案性能与通信开销与另外两个方案的进行了对比，如表 1 所示。其中 s 代表用户的属性个数，$|G|$ 代表 G 群中一个元素的长度。通常在可搜索加密方案中，通信开销主要是指密文长度，存储开销主要指密钥长度，本方案在通信开销上与 Wang[6]、Zheng[8]几乎一致，但是其存储开销是 Zheng[8]的一半。

表 1　方案性能的对比

方案	Wang[6]	Zheng[8]	本方案
隐藏访问结构	否	否	是
可搜索	是	是	是
可代理	否	否	是
关键字更新	否	否	是
访问结构	LSSS	树型	LSSS
密文长度	$(2l+1)\|G\|+\|G_T\|$	$(2l+1)\|G\|$	$(2l+4)\|G\|+\|G_T\|$
密钥长度	$(s+2)\|G\|$	$(2s+1)\|G\|$	$(s+2)\|G\|$

表 2 是本文方案与 Wang[6]、Zheng[8]进行计算开销的对比结果，其中 P 代表双线性操作，E 代表群 G 上的一次指数操作，E_T 代表群 G_T 上的一次指数操作，s 代表用户的属性个数，l 代表访问结构中的属性。由于哈希函数的计算量很小，所以本文在下面忽略了哈希函数的计算量。从表 2 可以看出本文的方案在密钥生成、密文生成、门限的生成阶段以及搜索阶段的计算开销都相对较小，可见本文在增加了隐藏访问结构与关键字更新功能的同时，方案的计算开销以及密文密钥的长度都未见明显增长，所以本方案具有很大的实用性。

表 2　计算开销的对比

方案	Wang[6]	Zheng[8]	本方案
密钥生成	$(s+2)E$	$(2s+2)E$	$(s+2)E$
密文生成	$P+3lE+2E_T$	$(2l+4)E$	$P+(2l+4)E$
门限生成	$(s+2)E$	$(2s+4)E$	$(s+4)E$
搜索	$(2l+1)P+lE_T$	$(2l+3)P+lE_T$	$(l+3)P+lE_T$

7 结束语

本文在现有的基于属性的可搜索加密的基础上，针对云计算环境中存在的安全存储、共享和搜索问题，提出了一种支持代理重加密的具有隐藏访问结构的功能基于属性的密文检索方案。不仅实现了隐私保护，还解决了授权用户不在线时，密文搜索以及密文解密权限委托给其他用户的问题，并且可支持关键字的更新。为了信息的有效共享，本文有效地结合了代理重加密，充分利用云系统的计算能力，由云系统利用授权用户提供的重加密密钥和新的关键字实现密文的转换，减轻了数据属主加密解密的负担，而且节省了本地存储以及管理维护的成本。通过通信开销和计算开销的对比可以看出本文加密、解密搜索效率较高，计算复杂度较小，所以本文具有较大的理论研究价值和实际应用价值。但是本方案未能考虑密文、密钥等消息长度随着属性的个数的增加而增加的问题，因此如何减少密文以及密钥的长度是本文今后需要进一步深入研究的问题。

chinaXiv:201804.02035v1

参考文献：

[1] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data [C]// Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 2000: 44.

[2] Dan B, Crescenzo G D, Ostrovsky R, et al. Public key encryption with keyword search [C]// Lecture Notes in Computer Science, vol 3027. 2004: 506-522.

[3] Golle P, Staddon J, Waters B. Secure conjunctive keyword search over encrypted data [J]// Lecture Notes in Computer Science, vol 3089. 2004: 31-45.

[4] Xu P, Jin H, Wu Q, et al. Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack [J]. IEEE Trans on Computers, 2013, 62 (11): 2266-2277.

[5] Wu T Y, Tsai T T, Tseng Y M, Efficient searchable ID-based encryption with a designated server [J]. Annals of Telecommunications, 2014, 69 (7): 391-402.

[6] Wang C, Li W, Li Y, et al. A ciphertext-policy attribute-based encryption scheme supporting keyword search function [C]// Cyberspace Safety and Security. 2013: 377-386.

[7] Kaushik K, Varadharajan V, Nallusamy R. Multi-user attribute based searchable encryption [C]// Proc of IEEE, International Conference on Mobile Data Management. 2013: 200-205.

[8] Waters B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [J]. Lecture Notes in Computer Science, vol 2008. 2011: 321-334.

[9] Zheng Q, Xu S, Ateniese G. VABKS: Verifiable attribute-based keyword search over outsourced encrypted data [C]// Proc of IEEE INFOCOM. 2014: 522-530.

[10] 李双，徐茂智. 基于属性的可搜索加密方案 [J]. 计算机学报, 2014 (5): 1017-1024.

[11] Sun W, Yu S, Lou W, et al. Protecting your right: Attribute-based keyword search with fine-grained owner enforced search authorization in the cloud [C]// Proc of IEEE INFOCOM. 2014: 226-234.

[12] Zhao F, Nishide T, Sakurai K. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control [C]// Proc of International Conference on Information Security and Cryptology. [S. l.] : Springer-Verlag, 2011: 406-418.

[13] Lai J, Deng R H, Li Y. Expressive CP-ABE with partially hidden access structures [C]// Proc of ACM Symposium on Information, Computer and Communications Security. New York: ACM Press, 2012: 18-19.

[14] Padhya M, Jinwala D. A novel approach for searchable CP-ABE with hidden Ciphertext-policy [C]// Proc of International Conference on Information Systems Security. 2014.

[15] Shao J, Cao Z, Liang X, et al. Proxy re-encryption with keyword search [J]. Information Sciences, 2010, 180 (13): 2576-2587.

[16] Mambo M, Okamoto E. Proxy cryptosystems: delegation of the power to decrypt ciphertexts (special section on cryptography and information security) [J]. IEICE Trans on Fundamentals of Electronics Communications & Computer Sciences, 1997, 80 (1): 54-63.

[17] Fang, Liming, Susilo, Willy, Ge, Chunpeng, et al. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search [J]. Theoretical Computer Science, 2012, 462 (1): 39-58.

[18] Wang X A, Huang X, Yang X, et al. Further observation on proxy re-encryption with keyword search [J]. Journal of Systems & Software, 2012, 85 (3): 643-654.

[19] Shi Y, Liu J, Han Z, et al. Attribute-based proxy re-encryption with keyword search. [J]. PLOS One, 2014, 9 (12): e116325.

[20] Liang K, Susilo W. Searchable Attribute-based mechanism with efficient data sharing for secure cloud storage [J]. IEEE Trans on Information Forensics & Security, 2015, 10 (9): 1981-1992.